

| | | |
|---|---|----------------------------|
| In the Matter of |) | |
| |) | |
| Rules and Regulations Implementing the |) | CG Docket No. <u>04-53</u> |
| Controlling the Assault of Non-Solicited |) | |
| Pornography and Marketing Act of 2003 |) | |
| |) | |
| Rules and Regulations Implementing the |) | CG Docket No. 02-278 |
| Telephone Consumer Protection Act of 1991 |) | |
| |) | |

Released: March 19, 2004

| | <u>Paragraph</u> |
|---|------------------|
| I. INTRODUCTION..... | 1 |
| II. BACKGROUND..... | 3 |
| A The CAN-SPAM Act | 3 |
| B The Telephone Consumer Protection Act | 5 |
| III. NOTICE OF PROPOSED RULEMAKING IN CG DOCKET NO. 04-53 | 7 |
| A Background | 7 |
| B Definition of Mobile Service Commercial Message. | 8 |
| 1 Commercial Electronic Mail Message | 9 |
| 2 Transmitted Directly to a Wireless Device Used by a Subscriber of Commercial Mobile Service | 12 |

E. Regulatory Flexibility Analysis

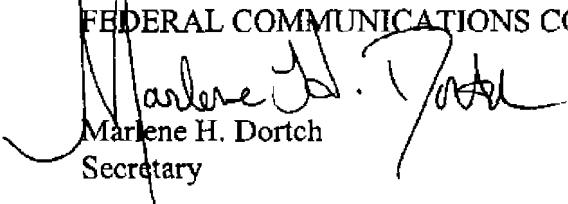
62 Pursuant to the Regulatory Flexibility Act of 1980, as amended,¹¹⁶ the Commission's Initial Regulatory Flexibility Analysis is attached as Appendix A

VI. ORDERING CLAUSES

63. Accordingly, IT IS ORDERED that, pursuant to the authority contained in sections 1-4, 227 and 303(r) of the Communications Act of 1934, as amended; the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699; and the Do-Not-Call Implementation Act, Pub. L. No. 108-10, 117 Stat. 557; 47 U.S.C. §§ 151-154, 227 and 303(r), the NOTICE OF PROPOSED RULEMAKING AND FURTHER NOTICE OF PROPOSED RULEMAKING ARE ADOPTED.

64 IT IS FURTHER ORDERED that the Commission's Consumer & Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Notice of Proposed Rulemaking and Further Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration

FEDERAL COMMUNICATIONS COMMISSION


Marlene H. Dortch
Secretary

¹¹⁶ 5 U.S.C. §§ 601 *et seq*

| | | |
|------------|--|-----------|
| C | The Ability to Avoid Receiving MSCMs..... | 18 |
| 1 | How to Enable Consumers to Avoid Unwanted MSCMs | 18 |
| 2 | Express Prior Authorization | 35 |
| 3 | Electronically Rejecting Future MSCMs | 37 |
| 4. | Exemption for Providers of Commercial Mobile Services | 38 |
| D. | Senders of MSCMs and the CAN-SPAM Act in General..... | 41 |
| IV. | FURTHER NOTICE OF PROPOSED RULEMAKING IN | |
| | CG DOCKET NO. 02-278..... | 43 |
| A. | Safe Harbor for Calls to Wireless Numbers..... | 43 |
| 1. | Background | 43 |
| 2 | Discussion | 46 |
| B. | National Do-Not-Call Registry and Monthly Updates By Telemarketers | 50 |
| 1 | Background | 50 |
| 2 | Discussion | 52 |
| V. | PROCEDURAL ISSUES..... | 54 |
| A. | Ex Parte Presentations..... | 54 |
| B. | Paperwork Reduction Act | 55 |
| C. | Filing of Comments and Reply Comments | 56 |
| D | Accessible Formats | 62 |
| E | Regulatory Flexibility Analysis | 63 |
| VI. | ORDERING CLAUSES..... | 64 |

APPENDIX A: INITIAL REGULATORY FLEXIBILITY ANALYSIS

I. INTRODUCTION

1 In this Notice of Proposed Rulemaking (Notice) we initiate a proceeding to implement the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act or Act).¹ The CAN-SPAM Act directs the Federal Communications Commission (FCC or Commission) to issue implementing regulations to protect consumers from unwanted mobile service commercial messages.² We seek comment on how to best carry out our mandate from Congress to protect consumers and businesses from the costs, inefficiencies and inconveniences that result from unwanted messages sent to their wireless devices.

2 In the Further Notice of Proposed Rulemaking (Further Notice) we seek further comment on the restrictions under the Telephone Consumer Protection Act (TCPA) on autodialed and artificial or prerecorded message calls to wireless telephone numbers.³ To ensure that telemarketers have reasonable opportunities to comply with the rules, we seek comment on

¹ Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (*CAN-SPAM Act*).

² See *CAN-SPAM Act*, Section 14(b).

³ Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (1991), *codified at* 47 U.S.C. § 227 (*TCPA*). The TCPA amended Title II of the Communications Act of 1934, 47 U.S.C. §§ 201 *et seq*.

2003, and/or CG Docket No. 02-278 for Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991. In completing the transmittal screen, commenters should include their full name, U.S. Postal Service mailing address, and the applicable docket or rulemaking number. Parties may also submit an electronic comment by Internet e-mail. To get filing instructions for e-mail comments, commenters should send an e-mail to ecfs@fcc.gov, and should include the following words in the body of the message, "get form." A sample form and directions will be sent in reply.

58. Parties who choose to file by paper must file an original and four copies of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, commenters must submit two additional copies for each additional docket or rulemaking number. Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail (although we continue to experience delays in receiving U.S. Postal Service mail).

59. The Commission's contractor, Natek, Inc., will receive hand-delivered or messenger-delivered paper filings for the Commission's Secretary at 236 Massachusetts Avenue, N.E., Suite 110, Washington, D.C. 20002. The filing hours at this location are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes must be disposed of before entering the building. Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743. U.S. Postal Service first-class mail, Express Mail, and Priority Mail should be addressed to 445 12th Street, S.W., Washington, D.C. 20554. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission. Parties who choose to file paper comments also should send four paper copies of their filings to Kelli Farmer, Federal Communications Commission, Room 4-C734, 445 12th Street, SW, Washington, DC 20554.

60. One copy of each filing must be sent to Qualex International, Portals II, 445 12th Street, S.W., Room CY- B402, Washington, D.C. 20554, telephone 202- 863- 2893, facsimile 202-863-2898, or via e-mail qualexint@aol.com. Filings and comments may be downloaded from the Commission's ECFS web site, and filings and comments are available for public inspection and copying during regular business hours at the FCC Reference Information Center, Portals II, 445 12th Street, SW, Room CY- A257, Washington, D.C. 20554. They may also be purchased from the Commission's duplicating contractor, Qualex International, which can be reached at Portals II, 445 12th Street, SW, Room CY- B402, Washington, D.C. 20554, by telephone at 202- 863- 2893, by facsimile at 202- 863- 2898, or via e-mail at qualexint@aol.com.

D. Accessible Formats

61. To request materials in accessible formats (computer diskettes, large print, audio recording and Braille) for persons with disabilities, contact the Consumer & Governmental Affairs Bureau, at (202) 418-0531, TTY (202) 418-7365, or at fcc504@fcc.gov.

adopting a limited "safe harbor" for telemarketers that call telephone numbers that have recently been ported from a wireline telecommunications provider to a wireless telecommunications provider. In addition, we seek comment in the Further Notice on whether we should amend our safe harbor provision for telemarketers that are required to comply with the national do-not-call registry. In an effort to remain consistent with the FTC's possible rule change, we propose amending our safe harbor to require telemarketers to update their call lists every 30 days.⁴

II. BACKGROUND

A. The CAN-SPAM Act

3. On December 8, 2003, Congress passed the CAN-SPAM Act to address the growing number of unwanted commercial electronic mail messages, which Congress determined to be costly, inconvenient, and often fraudulent or deceptive.⁵ Congress found that recipients "who cannot refuse to accept such mail" may incur costs for storage, and "time spent accessing, reviewing, and discarding such mail."⁶ The Act prohibits any person from transmitting such messages that are false or misleading and gives recipients the right to decline to receive additional messages from the same source.⁷ The Federal Trade Commission (FTC) and the Department of Justice (DOJ) are charged with general enforcement of the CAN-SPAM Act.⁸ Certain other agencies, including the FCC, are authorized to enforce the provisions of the Act with regard to entities under their jurisdiction.⁹ The FCC has such authority "with respect to any person subject to the Communications Act of 1934," and may do so with respect to others under "any other authority conferred on it by law."¹⁰

4. The CAN-SPAM Act requires the FCC to issue rules with regard to mobile service commercial messages within 270 days of January 1, 2004, and, in doing so, to consult and coordinate with the FTC.¹¹ Specifically, section 14 of the Act requires the FCC to promulgate rules to protect consumers from unwanted mobile service commercial messages, and in doing so, consider, among other factors, the ability of senders to determine whether a message is a mobile commercial electronic mail message.¹² In addition, the Act requires that in

⁴ See Consolidated Appropriations Act of 2004, Pub. L. No. 108-199, 188 Stat. 3 (*Appropriations Act*). This requirement is in Division B, Title V.

⁵ See *CAN-SPAM Act*, Section 2(a).

⁶ See *CAN-SPAM Act*, Section 2(a). Congress also found that the growth of unsolicited commercial electronic mail "imposes significant monetary costs" on Internet access service providers. *CAN-SPAM Act*, Section 2(a)(6).

⁷ *CAN-SPAM Act*, Section 5 (prohibiting false or misleading header information and subject lines). Section 4 of the Act also provides criminal sanctions for certain fraudulent activity in connection with sending electronic messages which Congress found to be particularly egregious. *CAN-SPAM Act*, Section 4.

⁸ See *CAN-SPAM Act*, Sections 7(a) and 4.

⁹ *CAN-SPAM Act*, Section 7(b) and (c). In addition, under section 7(f) States may, on behalf of their citizens, bring civil action seeking damages and injunctive relief against those who violate the section 5 of the Act.

¹⁰ *CAN-SPAM Act*, Section 7(b)(10) and (c).

¹¹ See *CAN-SPAM Act*, Section 14.

¹² See *CAN-SPAM Act*, Section 14(b) and (c). The Act defines "mobile service commercial message" as a "commercial electronic mail message that is transmitted directly to a wireless device that is utilized by a subscriber

(continued . . .)

rules? Are there any reasons the Commission should not amend its rules to be consistent with the FTC?

V. PROCEDURAL ISSUES

A. Ex Parte Presentations

54. This is a non-restricted notice and comment rulemaking proceeding. Ex parte presentations are permitted, except during the Sunshine Agenda period, provided that presentations are disclosed as provided in the Commission's rules.¹¹⁵

B. Paperwork Reduction Act

55. This Notice and Further Notice contains either proposed or modified information collections. As part of a continuing effort to reduce paperwork burdens, we invite the general public and the Office of Management and Budget (OMB) to take this opportunity to comment on the information collections contained in this Notice and Further Notice, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. Public and agency comments are due at the same time as other comments on this Notice and Further Notice; OMB comments are due 60 days from the date of publication of this Notice and Further Notice in the Federal Register. Comments should address: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; and (d) ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology.

C. Filing of Comments and Reply Comments

56. We invite comment on the issues and questions set forth above. Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 C.F.R. §§ 1.415, 1.419, interested parties may file comments in CG Docket No. 04-53, concerning unwanted mobile service commercial messages and the CAN-SPAM Act, on or before 30 days after publication in the Federal Register, and reply comments on or before 45 days after publication in the Federal Register. Parties shall file comments in CG Docket No. 02-278, concerning both a limited safe harbor under the TCPA and the required frequency for telemarketers to access the national do-not-call registry, on or before 15 days after publication in the Federal Register, and reply comments on or before 25 days after publication in the Federal Register.

57. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS) or by filing paper copies. See *Electronic Filing of Documents in Rulemaking Proceedings*, 63 Fed. Reg. 24121 (1998). Comments filed through the ECFS can be sent as an electronic file via the Internet at <<http://www.fcc.gov/e-file/ecfs.html>>. Generally, only one copy of an electronic submission must be filed. **Please make sure to file comments in the appropriate docket number:** either CG Docket No. 04-53 for Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of

¹¹⁵ See generally 47 C.F.R. §§ 1.1202, 1.1203, 1.1206(a).

promulgating its rules the Commission must provide subscribers the ability to avoid receiving mobile service commercial messages sent without the subscribers' prior consent, and the ability to indicate electronically a desire not to receive future mobile service commercial messages.¹³ Further the Act requires the Commission to consider the relationship that exists between providers of such services and their subscribers, as well as the ability of senders to comply with the requirements of the Act given the unique technical limitations of wireless devices.¹⁴ Finally, for purposes of this discussion, the CAN-SPAM Act also provides that "[n]othing in this Act shall be interpreted to preclude or override the applicability" of the TCPA.¹⁵

B. The Telephone Consumer Protection Act

5 The TCPA was enacted to address certain telemarketing practices, including calls to wireless telephone numbers, which Congress found to be an invasion of consumer privacy and even a risk to public safety.¹⁶ The statute restricts the use of automatic telephone dialing systems, artificial and prerecorded messages, and telephone facsimile machines to send unsolicited advertisements.¹⁷ The TCPA specifically prohibits calls using an autodialer or artificial or prerecorded message "to any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other common carrier service, or any service for which the called party is charged."¹⁸ In addition, the TCPA required the Commission to "initiate a rulemaking proceeding concerning the need to protect residential telephone subscribers' privacy rights" and to consider several methods to accommodate telephone subscribers who do not wish to receive unsolicited advertisements.¹⁹

6. In 2003, the Commission released a Report and Order revising the TCPA rules to respond to changes in the marketplace for telemarketing.²⁰ Specifically, we established, in conjunction with the FTC, a national do-not-call registry for consumers who wish to avoid unwanted telemarketing calls.²¹ The national do-not-call registry supplements long-standing company-specific rules which require companies to maintain lists of consumers who have directed the company not to contact them. We also determined that the TCPA prohibits *any call*

(continued from previous page)

of commercial mobile service" in connection with such service. See *supra* para 9, see also *CAN-SPAM Act*, Section 14(d).

¹³ See *CAN-SPAM Act*, Section 14(b)(1).

¹⁴ *CAN-SPAM Act*, Section 14(b)(3) and (4).

¹⁵ *CAN-SPAM Act*, Section 14(a); see also TCPA, Pub L No 102-243, 105 Stat 2394 (1991), codified at 47 U.S.C. § 227.

¹⁶ See TCPA, Section 2(5), reprinted in 7 FCC Rcd 2736 at 2744.

¹⁷ 47 U.S.C. § 227(b)(1).

¹⁸ 47 U.S.C. § 227(b)(1)(A)(iii).

¹⁹ 47 U.S.C. § 227(c)(1)-(4).

²⁰ See *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 18 FCC Rcd 14014 (2003) (2003 TCPA Order).

²¹ The United States Court of Appeals for the Tenth Circuit recently upheld the constitutionality of the national do-not-call registry. See *Mainstream Marketing Services, Inc v Federal Trade Commission*, No 03-1429 (10th Cir February 17, 2004).

safe harbor that the three-month period for telemarketers might prove to be too long to benefit some consumers, and indicated our intention to carefully monitor the impact of the requirement¹⁰⁹

51. On January 23, 2004, the Consolidated Appropriations Act of 2004 (Appropriations Act) was signed into law. The legislation mandated that “not later than 60 days after the date of enactment of this Act, the Federal Trade Commission shall amend the Telemarketing Sales Rule to require telemarketers subject to the Telemarketing Sales Rule to obtain from the Federal Trade Commission the list of telephone numbers on the ‘do-not-call’ registry once a month.”¹¹⁰ The FTC released a Notice of Proposed Rulemaking on February 10, 2004, proposing to amend its safe harbor provision under the Telemarketing Sales Rule so that telemarketers and sellers will need to purge from their calling lists numbers appearing on the national do-not-call registry every thirty (30) days, rather than quarterly.¹¹¹

2. Discussion

52. We seek comment on whether we should amend our safe harbor provision to mirror any amendment made by the FTC to its safe harbor. The Appropriations Act does not require the FCC to amend its rules. However, in the Do-Not-Call Implementation Act (Do-Not-Call Act), Congress directed the FCC to consult and coordinate with the FTC to “maximize consistency” with the rules promulgated by the FTC.¹¹² In addition, we note that, absent action to amend our safe harbor, many telemarketers will face inconsistent standards because the FTC’s jurisdiction extends only to certain entities, while our jurisdiction extends to all telemarketers.¹¹³

53. Therefore, in an effort to remain consistent with the FTC’s rules, we propose amending our safe harbor to require sellers and telemarketers acting on behalf of sellers to use a version of the national do-not-call registry obtained from the administrator of the registry no more than 30 days prior to the date any call is made. We seek comment on how amending our safe harbor provision, or failing to do so, would affect telemarketers’ ability to comply with the Commission’s do-not-call rules. What problems will telemarketers, including small businesses, face in “scrubbing”¹¹⁴ their call lists every 30 days that they do not experience under the current

(continued from previous page)

established pursuant to the do-not-call rules, (iii) the seller, or telemarketer acting on behalf of the seller, has maintained and recorded a list of telephone numbers the seller may not contact, and (iv) any subsequent call otherwise violating the do-not-call rules is the result of error. See 47 C.F.R. § 64.1200(c)(2)(i)

¹⁰⁹ See 2003 *TCPA Order*, 18 FCC Rcd at 14040, para. 38.

¹¹⁰ *Appropriations Act*. This requirement is in Division B, Title V.

¹¹¹ See *Telemarketing Sales Rule, Notice of Proposed Rulemaking*, Federal Trade Commission, 69 Fed. Reg. 7330-01, (February 13, 2004) (*FTC NPRM*). The FTC’s proposal employs the phrase “thirty (30) days,” rather than the term used in the statute, “monthly,” noting that “thirty (30) days” achieves greater clarity and precision in effectuating Congress’s intent in the Appropriations Act.

¹¹² *Do-Not-Call Act*, Section 3.

¹¹³ The FTC’s rules do not extend to entities over which it has no jurisdiction, including common carriers, banks, credit unions, savings and loans, companies engaged in the business of insurance, and airlines. They also do not apply to intrastate telemarketing calls.

¹¹⁴ “Scrubbing” refers to comparing a do-not-call list to a company’s call list and eliminating from the call list the telephone numbers of consumers who have registered a desire not to be called.

using an automatic telephone dialing system or an artificial or prerecorded message to any wireless telephone number.²² We concluded that this encompasses both voice calls and text calls to wireless numbers including, for example, Short Message Service (SMS) calls.²³ As part of our rulemaking, we also acknowledged that, beginning November 24, 2003, local number portability (LNP) would permit subscribers to port numbers previously used for wireline service to wireless service providers, and that telemarketers would need to take the steps necessary to ensure continued compliance with the TCPA.²⁴ In adopting rules, we concluded that a seller or the entity telemarketing on behalf of the seller will not be liable for violating the national do-not-call rules if it can demonstrate that it meets our safe harbor, including the requirement of accessing the national do-not-call database on a quarterly basis.²⁵

III. NOTICE OF PROPOSED RULEMAKING IN CG DOCKET NO. 04-53

A. Background

7. Section 14 of the CAN-SPAM Act requires the FCC, in consultation with the FTC, to issue rules to protect consumers from unwanted mobile service commercial messages by September 26, 2004.²⁶ Specifically, section 14(b), (c) and (d) of the CAN-SPAM Act provides that:

(b) FCC RULEMAKING — The Federal Communications Commission, in consultation with the Federal Trade Commission, shall promulgate rules within 270 days to protect consumers from unwanted mobile service commercial messages. The Federal Communications Commission, in promulgating the rules, shall, to the extent consistent with subsection (c) —

- 1) provide subscribers to commercial mobile services the ability to avoid receiving mobile service commercial messages unless the subscriber has provided express prior authorization to the sender, except as provided in paragraph (3);
- 2) allow recipients of mobile service commercial messages to indicate electronically a desire not to receive future mobile service commercial messages from the sender;
- 3) take into consideration, in determining whether to subject providers of commercial mobile services to paragraph (1), the relationship that exists between providers of such services and their subscribers, but if the Commission determines that such providers should not be subject to paragraph (1), the rules shall require such providers, in addition to complying with the other provisions of this Act, to allow subscribers to indicate a desire not to receive future mobile service commercial messages from the provider —

²² 2003 TCPA Order, 18 FCC Rcd at 14115, para. 165

²³ See *Id.*

²⁴ *Id.* at 14117, para. 170 LNP “means the ability of users of telecommunications services to retain, at the same location, existing telecommunications numbers without impairment of quality, reliability, or convenience when switching from one telecommunications carrier to another” 47 U.S.C. § 153(30). See also 47 C.F.R. § 52.21(k). Wireless carriers began providing LNP on November 24, 2003.

²⁵ 47 C.F.R. § 64.1200(c)(2)(i)(D)

²⁶ See CAN-SPAM Act, Section 14(b)

been in place for 12 years and the Commission's porting requirements have been in place for over five years.¹⁰⁴ Telemarketers have received sufficient notice of these requirements in order to develop business practices that will allow them to continue to comply with the TCPA. The record continues to demonstrate that information is currently available to assist telemarketers in determining which numbers are assigned to wireless carriers. Nevertheless, we recognize that once a number is ported to a wireless service, a telemarketer may not have access to that information immediately in order to avoid calling the new wireless number.

49. We seek comment on the narrow issue of whether the Commission should adopt a limited safe harbor during which a telemarketer will not be liable for violating the rule prohibiting autodialed and prerecorded message calls to wireless numbers once a number is ported from wireline to wireless service. If so, we seek comment on the appropriate safe harbor period given both the technical limitations on telemarketers and the significant privacy and safety concerns regarding calls to wireless subscribers.¹⁰⁵ For example, would a period of up to seven days be a reasonable amount of time for telemarketers to obtain data on recently ported numbers and to scrub their call lists of those numbers? Or, as the DMA has requested, should any safe harbor the Commission adopt provide telemarketers with up to 30 days to do so? Are there other options in the marketplace available to telemarketers that should affect whether we adopt a limited safe harbor as well as the duration of any such safe harbor?¹⁰⁶ We also seek comment on whether any safe harbor period adopted should sunset in the future and, if so, when. In addition, we seek comments from small businesses which engage in telemarketing about the appropriateness of such a limited safe harbor and its parameters.

B. National Do-Not-Call Registry and Monthly Updates By Telemarketers

1. Background

50. In adopting the national do-not-call registry, we determined that a safe harbor should be established for telemarketers that have made a good faith effort to comply with the national do-not-call rules.¹⁰⁷ Consistent with the actions of the FTC, we concluded that a seller or the entity telemarketing on behalf of the seller will not be liable for violating the national do-not-call rules if it can demonstrate that it meets certain standards, including accessing the national do-not-call database on a quarterly basis. To fall within this safe harbor, a telemarketer must use a process to prevent telephone solicitations to any telephone number on the national do-not-call list, "employing a version of the national do-not-call registry obtained from the administrator of the registry no more than three months prior to the date any call is made, and maintains records documenting this process."¹⁰⁸ We acknowledged at the time we adopted the

¹⁰⁴ See 2003 TCPA Order, 18 FCC Rcd at 14116, para. 168.

¹⁰⁵ See *Id.* at 14115, para. 164.

¹⁰⁶ See Letter from Dean Garfinkel, Chairman, Call Compliance, Inc. and Anthony Rutkowski, Vice President of Regulatory Affairs, VeriSign Communications Services to Marlene H. Dortch, Secretary, Federal Communications Commission, filed January 27, 2004.

¹⁰⁷ See 2003 TCPA Order, 18 FCC Rcd at 14040, para. 38. See also *Telemarketing Sales Rule, Final Rule*, Federal Trade Commission, 68 Fed. Reg. at 4645-46 (January 29, 2003).

¹⁰⁸ 47 C.F.R. § 64.1200(c)(2)(i)(D). The seller or telemarketer acting on behalf of the seller must also demonstrate that as part of its routine business practice, (i) it has established and implemented written procedures to comply with the do-not-call rules, (ii) it has trained its personnel, and any entity assisting in its compliance, in the procedures

(continued...)

- a at the time of subscribing to such service; and
 - b. in any billing mechanism, and
- 4) determine how a sender of mobile service commercial messages may comply with the provisions of this Act, considering the unique technical aspects, including the functional and character limitations, of devices that receive such messages.²⁷
- (c) **OTHER FACTORS TO BE CONSIDERED.** -- The Federal Communications Commission shall consider the ability of a sender of a commercial electronic mail message to reasonably determine that the message is a mobile service commercial message.²⁸
- (d) **MOBILE SERVICE COMMERCIAL MESSAGE DEFINED.** --In this section, the term "mobile service commercial message" means a commercial electronic mail message that is transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile services (as such term is defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d))) in connection with such service.²⁹

B. Definition of Mobile Service Commercial Message

8 Section 14(b)(1) of the CAN-SPAM Act states that the Commission shall adopt rules to provide subscribers with the ability to avoid receiving a "mobile service commercial message" (MSCM) unless the subscriber has expressly authorized such messages beforehand.³⁰ The Act defines an MSCM as a "commercial electronic mail message that is transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service" as defined in 47 U.S.C. § 332(d) "in connection with that service."³¹ For purposes of this discussion, we shall refer to mobile service messaging as MSM.³² As a threshold matter, we commence our inquiry by exploring the scope of messages covered by section 14.

1. Commercial Electronic Mail Message

9 Although the Act defines an electronic mail message broadly as a message having a unique electronic mail address with "a reference to an Internet domain," the scope of electronic messages covered under section 14 is narrowed.³³ MSCMs are only those electronic mail

²⁷ *CAN-SPAM Act*, Section 14(b)

²⁸ *CAN-SPAM Act*, Section 14(c).

²⁹ *CAN-SPAM Act*, Section 14(d)

³⁰ *CAN-SPAM Act*, Section 14(b)(1)

³¹ *CAN-SPAM Act*, Section 14(d).

³² As technology continues to develop and wireless and wireline systems converge, often there are multiple formats and devices available for viewing messages. When a customer subscribes to mobile service messaging, the subscription is to a system that transmits all types of messages, not just those of a commercial variety

³³ *CAN-SPAM Act*, Section 3(5) and (6) "Electronic mail message" is defined as "a message sent to a unique electronic mail address." *CAN-SPAM Act*, Section 3(6) An "electronic mail address" is further defined as "a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the 'local part') and a reference to an Internet domain (commonly referred to as the 'domain part'), whether or not displayed, to which an electronic mail message can be sent or delivered." *CAN-SPAM Act*, Section 3(5) and (6) An Internet domain reference, such as "fcc.gov," is used in standard addressing of electronic mail

Instead, we encouraged the telemarketing industry to make use of the tools available in the marketplace in order to ensure continued compliance with the TCPA.⁹⁷ Intermodal number portability went into effect on November 24, 2003, requiring carriers to allow consumers to transfer their telephone numbers from a wireline service to a wireless service provider.

45 Several parties raised concerns with the Commission about how to comply with the TCPA once intermodal LNP became effective.⁹⁸ The Direct Marketing Association (DMA) and Newspaper Association of America (NAA) submitted a Petition for Declaratory Ruling asking the Commission to adopt a safe harbor for calls made to any wireless number regardless of whether the number was recently ported to wireless service.⁹⁹ They argue that “inadvertent calls to wireless numbers are as inevitable as erroneous calls to numbers on the national Do-Not-Call list.”¹⁰⁰ Specifically, under the DMA and NAA’s “safe harbor” proposal, if a marketer subscribes to a wireless suppression service and uses a version of the data that is no more than 30 days old, the marketer will not be liable under the TCPA for erroneous calls to wireless numbers.¹⁰¹

2. Discussion

46. We now seek additional comment on the ability of telemarketers, especially small businesses, to comply with the TCPA’s prohibition on calls to wireless numbers since implementation of intermodal LNP. We specifically seek comment on whether the Commission should adopt a limited safe harbor for autodialed and prerecorded message calls to wireless numbers that were recently ported from a wireline service to a wireless service provider.

47 The DMA indicates that it is in the process of creating a ported number database.¹⁰² It contends, however, that this solution will not allow marketers to update their call lists instantaneously when consumers port their wireline numbers. The DMA argues that, even with a direct link to Neustar’s database of wireless service numbers that have recently been ported from wireline service, there will be time lags throughout the process, during which a consumer who has just ported a wireline number to wireless service could receive a call from a marketer.¹⁰³

48 As the Commission stated in the *2003 TCPA Order*, the TCPA rules prohibiting telemarketers from placing autodialed and prerecorded message calls to wireless numbers have

⁹⁷ *Id.* at 14117, para. 170, citing letter from Neustar to the Federal Communications Commission, filed June 4, 2003.

⁹⁸ See, e.g., Letter from Jerry Cerasale, Senior Vice President, Direct Marketing Association to K. Dane Snowden, FCC, December 2, 2003, and Letter from Anita Wallgren on behalf of the Tribune Company to Marlene H. Dortch, Secretary, Federal Communications Commission, filed November 10, 2003.

⁹⁹ See Petition for Declaratory Ruling, Direct Marketing Association and Newspaper Association of America, filed January 29, 2004 (*DMA Petition*).

¹⁰⁰ *DMA Petition* at 4.

¹⁰¹ See *DMA Petition* at 2. The DMA contends that, although the TCPA does not explicitly include a safe harbor for calls placed to wireless numbers, “there is significant ambiguity in the statute to allow the FCC to use its rulemaking authority to create one.” *DMA Petition* at 7.

¹⁰² See *DMA Petition* at 4.

¹⁰³ *Id.* at 4-5.

messages “transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service” as defined in 47 U.S.C. § 332(d) “in connection with that service.”³⁴ Section 332(d) defines the term “commercial mobile service” as a mobile service that is provided for profit and makes interconnected service available to the public or to such classes of eligible users as to be effectively available to a substantial portion of the public.³⁵ The Commission equates the statutory term “commercial mobile service” with “commercial mobile radio service” or CMRS used in its rules.³⁶

10 Accordingly, it appears that only commercial electronic messages transmitted directly to a wireless device used by a CMRS subscriber would fall within the definition of MSCMs under the Act. Further, we note that the Act states that an electronic mail message shall include a unique electronic mail address, which is defined to include two parts: 1) “a unique user name or mailbox;” and 2) “a reference to an Internet domain.”³⁷ Thus, it appears that MSCM would be limited under the Act, to a message that is transmitted to an electronic mail address provided by a CMRS provider for delivery to the addressee subscriber’s wireless device. We seek comment on this interpretation and its alternatives. Commenters should address whether only these or other messages would fall under the definition of MSCM.

11 Under the Act, whether an electronic mail message is considered “commercial” is based upon its “primary purpose.”³⁸ It meets this definition if its primary purpose is “the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose).”³⁹ A “commercial” message for purposes of the Act does not include a transactional or relationship message.⁴⁰ The Act requires the FTC to issue regulations defining the relevant criteria to facilitate the determination of the primary purpose of an electronic mail message by January of 2005.⁴¹

2. Transmitted Directly to a Wireless Device Used by a Subscriber of Commercial Mobile Service

12. As explained above, in order to satisfy the definition of an MSCM, the message

³⁴ *CAN-SPAM Act*, Section 14(d).

³⁵ 47 U.S.C. § 332(d).

³⁶ See *Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993 Annual Report and Analysis of Competitive Market Conditions with Respect to Commercial Mobile Services*, WT Docket No. 02-379, Eighth Report, FCC 03-150 at 3 n.1 (rel. July 14, 2003).

³⁷ *CAN-SPAM Act*, Section 3(5) and (6).

³⁸ *CAN-SPAM Act*, Section 3(2).

³⁹ *CAN-SPAM Act*, Section 3(2)(A); see also Section 3(2)(D).

⁴⁰ *CAN-SPAM Act*, Section 3(2)(B). Transactional and relationship messages include those sent regarding product safety or security information, and notification about changes in terms, features, or the customer’s status. See *CAN-SPAM Act*, Section 3(17)(A)(i)-(iii). See also Section 3(2)(D) (noting that a reference to a commercial entity does not by itself make a message a commercial message).

⁴¹ *CAN-SPAM Act*, Section 3(2)(C). See also *Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act*, Federal Trade Commission, 69 Fed. Reg. 11776 (March 11, 2004). In addition, the *CAN-SPAM Act* gives the FTC the ability to modify the exemptions. See *CAN-SPAM Act*, Section 3(17)(B) (expand or contract the categories of messages treated as transactional or relationship messages).

required identifier, material on how to request no more messages, and postal address), because that content might be limited in length or might not be readily displayable. Consequently, there might be some technical difficulties in ensuring that electronic mail content is provided to subscribers in compliance with the requirements of the Act. We seek comment on these issues, particularly as they affect small wireless providers and other small businesses. We ask for comment on whether any such issues will be mitigated in the near future with advances in technology. For example, we understand that some commercial mobile service subscribers may already supplement the limited text handling functionality with ancillary personal computer technology.⁹⁰ We seek comment on this and any other possible technical considerations for senders of MSCMs that must comply with the Act.

IV. FURTHER NOTICE OF PROPOSED RULEMAKING IN CG DOCKET NO. 02-278

A. Safe Harbor for Calls to Wireless Numbers

1. Background

43. As discussed above, the TCPA restricts, among other things, the use of automatic telephone dialing systems and prerecorded messages.⁹¹ The statute specifically prohibits calls using an autodialer or artificial or prerecorded message “to any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other common carrier service, or any service for which the called party is charged.”⁹² On July 3, 2003, we released a Report and Order in which we determined that under the TCPA, “it is unlawful to make *any call* using an automatic telephone dialing system or an artificial or prerecorded message to any wireless telephone number”⁹³

44. In addition, we acknowledged in the *2003 TCPA Order* that, beginning November 24, 2003, numbers previously used for wireline service could be ported to wireless service providers and that telemarketers will need to take the steps necessary to identify these numbers.⁹⁴ We also noted that information is available from a variety of sources to assist telemarketers in determining which numbers are assigned to wireless carriers.⁹⁵ Therefore, based on the evidence in the record, we found that it was not necessary to add rules to implement the TCPA as a result of the introduction of wireline to wireless number portability, known as intermodal LNP.⁹⁶

⁹⁰ See, e.g., “Use Bluetooth for SMS,” Wei-Meng Lee, (November 27, 2002) <www.oreillynet.com/lpt/a/2983> and “Sending SMS Messages Using Windows XP,” Wei-Meng Lee (October 10, 2003) <www.oreillynet.com/lpt/a/4230>

⁹¹ 47 U.S.C. § 227(b)(1)

⁹² 47 U.S.C. § 227(b)(1)(A)(iii). The prohibition excludes calls “made for emergency purposes or made with the prior express consent of the called party.” 47 U.S.C. § 227(b)(1)(A).

⁹³ *2003 TCPA Order*, 18 FCC Rcd at 14115, para 165.

⁹⁴ *Id.* at 14117, para 170. Wireless carriers began providing local number portability (LNP) on November 24, 2003. LNP “means the ability of users of telecommunications services to retain, at the same location, existing telecommunications numbers without impairment of quality, reliability, or convenience when switching from one telecommunications carrier to another.” 47 U.S.C. § 153(30). See also 47 C.F.R. § 52.21(k).

⁹⁵ *2003 TCPA Order*, 18 FCC Rcd at 14117, para 170.

⁹⁶ *Id.* at 14116, para 168.

must be “transmitted directly to a wireless device.” In light of the definition of an MSCM, as discussed above, it appears that the statutory language would be satisfied when a message is transmitted to an electronic mail address provided by a CMRS provider for delivery to the addressee subscriber’s wireless device. As discussed below, we believe that the specific transmission technique used in delivering a particular message may not be relevant under the statute, and that messages “forwarded” by a subscriber to his or her own wireless device are not covered under section 14. We seek comment on these interpretations as well as the issues described below.

13 We have asked above whether a message becomes an MSCM only if it is transmitted to a wireless device used by a subscriber of CMRS “in connection with that service.” We seek comment on whether an interpretation that all commercial electronic mail messages sent to CMRS carriers’ mobile messaging systems are MSCMs would be consistent with the definition of MSCM in the Act. For example, do CMRS carriers offer services through which electronic mail messages are sent directly to wireless devices other than in connection with commercial mobile service as defined in section 332(d)? Commenters should also discuss any other relevant issues involving the definition of MSCM.

14 *Transmission techniques.* Currently, there appear to be two main methods for transmitting messages to a wireless device, and those methods are through push and pull technologies. Message transmission techniques using “pull” technologies store messages on a server until a recipient initiates a request to access the messages from either a wireless or non-wireless device. “Push” technologies automatically – without action from the recipient – send messages to a recipient’s wireless device. Certain messages that are initiated as electronic mail messages on the Internet and converted for delivery to a wireless device, discussed below in the context of SMS messaging, are examples of messages delivered to wireless devices using such push technologies. We believe that the definition of a MSCM should include all messages transmitted to an electronic mail address provided by a CMRS provider for delivery to the addressee subscriber’s wireless device irrespective of the transmission technique. We seek comment on this interpretation and alternatives.

15. The legislative history of the Act suggests section 14, in conjunction with the TCPA, was intended to address wireless text messaging.⁴² SMS messages are text messages directed to wireless devices through the use of the telephone number assigned to the device. When SMS messages are sent between wireless devices, the messages generally do not traverse the Internet and therefore do not include a reference to an Internet domain. However, a message initially may be sent through the Internet as an electronic mail message, and then converted by the service provider into an SMS message associated with a telephone number.⁴³ We seek comment on whether the definition of an MSCM should include messages using such technology and similar methods, and specifically whether it should include either or both of these types of

⁴² See 149 Cong. Rec. H12186-02 at 12193 (Congressman Markey: “As we attempt to tackle the issue of spam that is sent to our desktop computer, we must also recognize that millions of wireless consumers in the United States run the risk of being inundated by wireless spam. Unsolicited wireless text messages have plagued wireless users in Europe, South Korea and Japan over the last few years as wireless companies in such countries have offered wireless messaging services.”) See also 149 Cong. Rec. H12854-08 at 12860.

⁴³ The address would contain a reference to an Internet domain. It could reference the subscriber’s assigned telephone number. For example, “2024189999@[wireless company name].com.”

is a need for a separate exemption for CMRS providers from the section 14 "express prior permission" requirement. In particular, we seek specific examples of messages, if any, that CMRS providers send to their customers that are not already excluded under the Act in general. Should any exemptions for carriers be limited to only those messages sent by CMRS carriers regarding their own service? What would be the impact of any such exemption on small businesses?

40 If the Commission opts to exempt CMRS carriers from obtaining prior express authorization, Congress has required that such providers, in addition to complying with other provisions of the Act, must allow subscribers to indicate a desire to receive no future MSCMs from the provider: 1) at the time of subscribing to such service and 2) in any billing mechanism.⁸⁴ We seek comment on how we might implement those requirements, if we provide an exemption. Finally, we seek comment regarding whether small wireless service providers should be treated differently with respect to any of these issues, and if so, how.

D. Senders of MSCMs and the CAN-SPAM Act in General

41. Section 14(b)(4) of the Act requires the Commission to determine how a sender of an MSCM may comply with the provisions of the CAN-SPAM Act in general, considering the "unique technical aspects, including the functional and character limitations, of devices that receive such messages."⁸⁵ If a sender is not prohibited from sending MSCMs to an address, either because the subscriber has not used his ability to stop such messages or because the sender has received "express prior authorization," then the message must still comply with the Act in general.⁸⁶ Therefore, we ask for comment on specific compliance issues that senders of MSCM might have with other sections of the Act.⁸⁷

42. We believe that a large segment of MSM subscribers who receive and send text-based messages on their wireless devices today do so on digital cellular phones that are designed principally for voice communications and that provide limited electronic mail message functionality. Currently, text messages are often limited to a maximum message length of ranging from 120 to 500 characters.⁸⁸ Some MSM providers limit the length of messages allowed on their systems to approximately 160 characters.⁸⁹ As a result, it might be difficult for senders to supply information required by the CAN-SPAM Act (such as header information and

⁸⁴ *CAN-SPAM Act*, Section 14(b)(3).

⁸⁵ *See CAN-SPAM Act*, Section 14(b)(4).

⁸⁶ We note also that the requirements of those sections would also apply if the definition we adopt for "express prior authorization" from Section 14 does not meet the standards of "affirmative consent" under the main Act. *See CAN-SPAM Act*, Sections 3(1), 4, 5, and 6.

⁸⁷ *See, e.g., CAN-SPAM Act*, Sections 4, 5 and 6.

⁸⁸ *See Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993 Annual Report and Analysis of Competitive Market Conditions with Respect to Commercial Mobile Services*, WT Docket No. 02-379, Eighth Report, FCC 03-150 at 64 (rel. July 14, 2003).

⁸⁹ *See, e.g.,* <www.vtext.com/customer_site/jsp/aboutservice.jsp>, <www.cingular.com/beyond_voice/tm_user/>, and <www.attwireless.com/personal/features/communication/howtotextmessage.jhtml>. For example, the precise number of characters conveyed in an SMS message may vary depending on the data encoding and access method used by the commercial mobile service.

SMS messages described above. We note here that the TCPA and Commission rules prohibit calls using autodialers to send certain voice calls and text calls, including SMS messages, to wireless numbers.⁴⁴

16 *Forwarding* The manner in which recipients of MSCMs utilize messaging options may also be relevant to our interpretation of the definition of MSCM. For example, another way for a commercial mobile service subscriber to obtain electronic mail messages is for that subscriber to take steps to have messages forwarded from a server to the subscriber's wireless device. With this type of electronic mail transmission, a subscriber can, for example, obtain messages initially sent to an electronic mail account that is normally accessed by a personal computer.⁴⁵ We do not believe that section 14 was intended to apply to all such messages. First, defining the scope of section 14 to include all "forwarded" messages could result in our rules applying to virtually all electronic mail covered by the CAN-SPAM Act because subscribers can forward most electronic mail to their wireless devices. We do not believe that Congress intended such a result given that it would duplicate in large measure the FTC's authority under the Act. Moreover, the legislative history of the Act suggests that section 14 was not intended to address messages "forwarded" in this manner.⁴⁶ Congressman Markey, in support of section 14, stated: "Spam sent to a desktop computer e-mail address, and which is then forwarded over to a wireless network to a wireless device, i.e., delivered 'indirectly' from the initiator to the wireless device, would be treated by the rest of this bill and not by the additional section 14 wireless-specific provisions we subject to an FCC rulemaking."⁴⁷ We seek comment on the view that such transmissions fall outside the category of those "transmitted directly to a wireless device." Commenters should address our assumption that a broad interpretation of "transmitted directly to a wireless device" to cover "forwarded" electronic mail messages would expand the scope of section 14 to cover all electronic mail covered by the CAN-SPAM Act in general.

17 Section 14 requires that the FCC "consider the ability of a sender of a commercial electronic mail message to reasonably determine that the message is a mobile service commercial message."⁴⁸ We seek comment on how a sender would know that it was sending an MSCM if any action by a recipient to retrieve his messages by a wireless device could convert a non-MSCM into an MSCM, or vice-versa. We seek comment on the technical and

⁴⁴ See *infra* paras. 43, see 2003 TCPA Order, 18 FCC Rcd at 14115, para 165 ("it is unlawful to make any call using an automatic telephone dialing system or an artificial or prerecorded message to any wireless telephone number"), see also 47 U.S.C. § 227(b)(1)(A)(iii) and 47 C.F.R. § 64.1200(a)(1)(iii).

⁴⁵ This type of transmission, employed in association with smart phones such as "Blackberry"-type devices, uses a server that can reside, for example, at the subscriber's work location. See <www.rim.com/>. In other cases, this type of service might be provided by the subscriber's wireless provider or other provider. Electronic mail obtained by these servers is periodically forwarded to the server maintained by the commercial mobile service provider and then sent to the subscriber's wireless device. Such server systems typically allow subscribers to create such instructions, "forwarding rules," independently, and to redirect messages.

⁴⁶ See 149 Cong. Rec. H12854-08 at 12860.

⁴⁷ See 149 Cong. Rec. H12854-08 at 12860 (Congressman Markey stated, "[T]his legislation now contains the Markey amendment on wireless spam, which originated in the House amendments to the Senate-passed bill. The reason I offered this amendment for inclusion in the House-passed bill is that I wanted wireless consumers to have greater protection than that which was accorded in the version of S. 877 which the Senate passed previously.)

⁴⁸ CAN-SPAM Act, Section 14(c).

comment on whether a challenge-and-response system, as discussed above, could be used to accomplish this goal.⁷⁸ A challenge-response mechanism sends back a challenge that requires a response verifying some aspect of the message. In addition to the challenge-response systems, could an MSM subscriber select a "secret code" or other personal identifier that a subscriber could distribute selectively to entities who she wanted to be able to send MSCMs to her? Could such an approach enable a carrier to filter out all commercial messages that do not include that "secret code" or personal identifier? We seek comment on whether there is some mechanism using the customer's wireless equipment, rather than the network, that could be used by a subscriber to screen out future MSCMs. We seek comment on these and any other methods that would allow the recipient of MSCMs to indicate electronically a desire not to receive future MSCMs from the sender. We especially seek comment from small businesses that might be affected by such a requirement. Further we seek comment on whether it would be appropriate to require or allow senders of MSCMs to give subscribers the option of going to an Internet website address provided by the sender to indicate their desire not to receive future MSCMs from the sender. Additionally, we seek comment on whether there are additional considerations needed for MSCMs sent to subscribers who are roaming on the network, given, for example, that different networks may have different technological capabilities.

4. Exemption for Providers of Commercial Mobile Services

38 Section 14(b)(3) requires the Commission to take into consideration whether to subject *providers* of commercial mobile services to paragraph (1) of the Act.⁷⁹ As a result, the Commission may exempt CMRS providers from the requirement to obtain express prior authorization from their current customers before sending them any MSCM. In making any such determination, the Commission must consider the relationship that exists between CMRS providers and their subscribers.⁸⁰

39. We seek comment on whether there is a need for such an exemption and how it would impact consumers.⁸¹ As discussed above, the Act already excludes certain "transactional and relationship" messages from the definition of unsolicited commercial electronic mail.⁸² These transactional and relationship messages include those sent regarding product safety or security information, notification to facilitate a commercial transaction, and notification about changes in terms, features, or the customer's status.⁸³ We seek comment then on whether there

⁷⁸ See *supra* para 32

⁷⁹ *CAN-SPAM Act*, Section 14(b)(3).

⁸⁰ *Id*

⁸¹ For example, in the 1992 *TCPA Order*, the Commission concluded that calls made by cellular carriers to their subscribers for which the subscribers were not charged do not fall within the TCPA's prohibitions on autodialers or prerecorded messages. The Commission believed that "neither TCPA nor the legislative history indicat[ed] that Congress intended to impede communications between radio common carriers and their customers regarding the delivery of customer services by barring calls to cellular subscribers for which the subscriber is not called [sic]." See *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CC Docket No. 92-90, Report and Order, 7 FCC Rcd 8752 at 8775, para 45 (1992) (*1992 TCPA Order*). In the 2003 *TCPA Order*, however, the Commission determined generally that wireless customers are charged for incoming calls whether they pay in advance or after the minutes are used. See 2003 *TCPA Order*, 18 FCC Rcd at 14115, para 165.

⁸² See *supra* para. 11. See also *CAN-SPAM Act*, Section 3(2)(B).

⁸³ See *CAN-SPAM Act*, Section 3(17)(A)(i)-(iii).

administrative characteristics relevant to distinguishing forwarded messages as well as other messages

C. The Ability to Avoid Receiving MSCMs

1. How to Enable Consumers to Avoid Unwanted MSCMs

18 We seek comment on ways in which we can implement Congress's directive to protect consumers from "unwanted mobile service commercial messages."⁴⁹ As explained above, section 14(b)(1) of the CAN-SPAM Act states that the Commission shall adopt rules to provide subscribers with the "ability to avoid receiving [MSCMs] unless the subscriber has provided express prior authorization to the sender."⁵⁰ The legislative history of the Act suggests that section 14 was included so that wireless subscribers would have greater protections from commercial electronic mail messages than those protections provided elsewhere in the Act.⁵¹ As explained below, we believe that section 14(b)(1) is intended to provide consumers the opportunity to generally bar receipt of all MSCMs (except those from senders who have obtained the consumer's prior express consent)⁵² However, we believe that in order to do so, the consumer must take affirmative action to bar the MSCMs in the first instance. Although it appears that Congress intended to afford wireless subscribers greater protection from unwanted commercial electronic mail messages than those protections provided elsewhere in the Act, it is not clear that Congress necessarily sought to impose a flat prohibition against such messages in the first instance. However, as set forth below, we seek comment on both of these different interpretations of section 14(b)(1).

19 The language of the CAN-SPAM Act requires the Commission to "protect consumers from unwanted mobile service commercial messages."⁵³ The protections extend to unwanted MSCMs from senders who may ignore the provisions of the CAN-SPAM Act. As a practical matter, the particular protections for wireless subscribers required by the Act may require comprehensive solutions. Therefore, in addition to those considerations directed by the CAN-SPAM Act discussed below, we seek comment generally on technical mechanisms that could be made available to wireless subscribers so that they may voluntarily, and at the subscriber's discretion, protect themselves against unwanted mobile service commercial

⁴⁹ See *CAN-SPAM Act*, Section 14(b), which provides, "[t]he Federal Communications Commission, in consultation with the Federal Trade Commission, shall promulgate rules within 270 days to protect consumers from unwanted mobile service commercial messages."

⁵⁰ *CAN-SPAM Act*, Section 14(b)(1). Section 14(b)(1) recognizes the potential for an exception to this prior authorization requirement in the relationship between the subscriber and their commercial mobile service provider. *CAN-SPAM Act*, Section 14(b)(3).

⁵¹ See 149 Cong. Rec. H12854-08 at 12860 (Congressman Markey states "in order to safeguard consumer privacy in a way that reflects the more intrusive nature of wireless spam to the user than spam to a desktop computer, which is immobile and for which the user may pay some type of 'per message' fee, the bill tasks the FCC with tackling this issue now, before it overwhelms users and network operators alike. . . . Section 14 of the bill builds upon this legislative foundation and puts in place additional protections and modifications. It requires an FCC rulemaking to assess and put in place additional consumer protections.") See also 149 Cong. Rec. H12186-02 at 12193.

⁵² Section 14 allows the Commission to exempt providers of commercial mobile services from this express prior authorization requirement. See *CAN-SPAM Act*, Section 14(b)(3), see also *infra* paras. 38-40.

⁵³ *CAN-SPAM Act*, Section 14(b).

avoid receiving MSCMs, unless the subscriber has provided express prior authorization to the sender.⁷¹ We seek comment on the form and content of such “express prior authorization.” We seek comment on whether it should be required to be in writing, and how any such requirement could be met electronically.⁷² We note that certain other requirements of the Act do not apply if the sender has obtained the subscriber’s “affirmative consent.”⁷³ As defined in the Act, “affirmative consent” means: 1) that the recipient expressly consented either in response to a clear and conspicuous request for such consent, or at the recipient’s own initiative; and 2) in cases when the message is from a party other than the party which received consent, that the recipient was given clear and conspicuous notice at the time of consent that the electronic mail address could be transferred for the purpose of initiating commercial e-mail messages.⁷⁴ We seek comment on whether the definition of “affirmative consent” would also be suited to use in defining “express prior authorization.”

36 We seek comment on whether any additional requirements are needed and the technical mechanisms that a subscriber could use to give express prior authorization. For example, should there be a notice to the recipient about the possibility that costs could be incurred in receiving any message?⁷⁵ What technical constraints imposed by the unique limitations of wireless devices are relevant in considering the form and content of express prior authorization.⁷⁶ We seek comment on ways to ease the burdens on both consumers and businesses, especially small businesses, of obtaining “express prior authorization” while maintaining the protections intended by Congress.

3. Electronically Rejecting Future MSCMs

37 Section 14(b)(2) specifically requires that we develop rules that “allow recipients of MSCMs to indicate electronically a desire not to receive future MSCMs from the sender.”⁷⁷ We seek comment on whether there are any technical options that might be used, such as a code that could be entered by the subscriber on her wireless device to indicate her withdrawal of permission to receive messages. For example, could an interface be accessed over the Internet (not necessarily through the wireless device) so that a user would access his or her account and modify the senders’ addresses for which messages would be blocked or allowed through? We seek comment on whether carriers, especially small carriers, already have systems in place to allow subscribers to block messages from a sender upon request of a subscriber. We also seek

⁷¹ *CAN-SPAM Act*, Section 14(b)(1)

⁷² The Electronic Signatures in Global and National Commerce Act, S.761, codified at 15 U.S.C. § 7001 (E-Sign Act) states that notwithstanding any regulation, or other rule of law with respect to any transaction in or affecting interstate or foreign commerce, a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and, further, a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation. *E-sign Act*, 15 U.S.C. § 7001(a)

⁷³ See, e.g., *CAN-SPAM Act*, Section 5.

⁷⁴ *CAN-SPAM Act*, Section 3(1).

⁷⁵ See, e.g., 47 C.F.R. § 64.1504(c)(2) (noting disclosure requirements for pay-per-call)

⁷⁶ We discuss the compliance of senders with the requirements of the CAN-SPAM Act given the “unique technical aspects” of devices receiving MSCM. See *infra* Part 3 D.

⁷⁷ *CAN-SPAM Act*, Section 14(b)(2)

messages. We seek comment on means by which wireless providers might protect consumers from MSCMs transmitted by senders who may willfully violate the wireless provisions of the CAN-SPAM Act addressed in this proceeding. We seek comment on how, in particular, small businesses would be affected by the various proposals we consider.

20. We are aware that a number of other countries have taken a variety of technical and regulatory steps to protect their consumers from unwanted electronic mail messages in general. In doing so, some countries such as Japan and South Korea have adopted an opt-out approach; while others such as the United Kingdom, France, and Germany had adopted an opt-in approach. Still others have a mixed approach. Also, different countries have taken a variety of positions on whether labeling and identification of commercial messages is required, whether a Do-Not-E-Mail registry can be developed, and whether the use of "spamware" is prohibited.⁵⁴ We seek comment on any of these approaches, consistent with section 14, applicable to unwanted mobile service commercial messages, with particular emphasis on their effectiveness, associated costs and burdens, if any, on carriers, subscribers or other relevant entities. Commenters should not only focus on the present, but also on the foreseeable future.

a. Prohibiting the Sending of MSCMs

21. Section 14(b)(1) states that the Commission's rules shall "provide subscribers to commercial mobile services the ability to avoid receiving mobile service commercial messages unless the subscriber has provided express prior authorization to the sender." One possible interpretation of this provision is that Congress intended to prohibit all senders of commercial electronic mail from sending MSCMs unless the senders first obtain express authorization from the recipient. This reading would allow the subscriber to avoid all MSCMs unless the subscriber acts affirmatively to give express permission for messages from individual senders.

22. Another interpretation of this provision is that Congress intended the subscriber to take affirmative steps to avoid receiving MSCMs to indicate his or her desire not to receive such messages. For example, under this interpretation, the customer might, at the time he or she subscribes to the mobile service, affirmatively decline to receive MSCMs. The subscriber would still have the option to agree to accept MSCMs from particular senders. We invite comment on both interpretations, particularly in light of the technological abilities and any constitutional concerns.⁵⁵

23. We also ask for comment on the practical aspects of either interpretation of this provision, given potential problems senders might have currently in determining whether the

⁵⁴ See "Background Paper for the OECD Workshop on Spam," Organization of Economic Cooperation and Development, January 22, 2004 <www.oecd.org>. For a discussion of the Do-Not-E-Mail registry, see *supra* para 29.

⁵⁵ We note that in enacting the CAN-SPAM Act, Congress found that "there is a substantial government interest in regulation of commercial electronic mail on a nationwide basis." See *CAN-SPAM Act*, Section 2(b). The findings of Congress included that electronic mail has become an extremely important and popular means of communication, that the convenience and efficiency of electronic mail are threatened by the high volume of unsolicited commercial electronic mail, that the receipt of unsolicited commercial electronic mail may result in costs for storage and/or time spent accessing, reviewing, and discarding such mail, and that the growth in such electronic mail imposes significant monetary costs on providers of Internet access services, businesses, and educational and nonprofit institutions. See *CAN-SPAM Act*, Section 2(a)(1) through (3) and (6).

recipient was an MSM subscriber.⁶⁶ Data suggests that this “challenge-response” approach is available in countering unwanted electronic mail, and a number of variants are possible.⁶⁷ We seek comment on such mechanisms and alternatives. Is it reasonable to expect the sender to note the addressee’s status and refrain from sending future messages to that address unless the sender has prior express authorization? Could mechanisms notifying the sender after he has sent an MSCM serve as an alternative or supplement to other mechanisms for enabling the sender to identify MSM subscriber addresses before an MSCM is sent? Would this practice be less burdensome to small businesses than alternative proposals? Would a challenge-response mechanism designed to filter out commercial electronic mail present an inappropriate impediment to non-commercial messages?

c. Commercial Message Identification

33 We note that, in order to make any blocking or filtering mechanisms respond only to commercial messages, rather than to all messages, commercial messages would first need to be identified.⁶⁸ We seek comment on the best methods that could be used by an MSM provider to identify such messages as commercial, if such methods are needed to make a filtering system effective. For example, would it be useful to use characters at the start of the subject line, or other methods? We seek comment on methods for “tagging” such messages so that they are identifiable as commercial messages. In addition, we ask about the practicality of having an MSM provider automatically request a response from the sender’s server for any MSCMs identified by unique characters in the subject line labeling.⁶⁹ We seek comment on this and other similar approaches and their respective merits and practicality. We seek comment on specific alternative approaches.

34 By itself, a prohibition against anyone sending MSCMs without prior express permission would place the burden on the sender to ensure that it is not sending its messages to MSM addresses. We seek comment therefore on whether it would be necessary or useful to consider the option of “tagging” commercial messages to identify them. We seek comment on this issue and on our authority to require such tagging on all commercial electronic mail. We note that the Act requires the FTC to tender a report to Congress outlining a plan to address the labeling of commercial electronic mail messages in general.⁷⁰ We are especially interested in the comments of small businesses about this alternative. Is it less burdensome than other alternatives?

2. Express Prior Authorization

35 Congress directed the FCC to adopt rules to provide consumers with the ability to

⁶⁶ For example, such a response might require confirmation of the sender’s awareness and intent before continuing delivery processing.

⁶⁷ See, e.g., “Controlling e-mail spam,” <spam_abuse_net/adminhelp/mail.shtml> (noting the NAGS Spam Filter can reject spam mail automatically, sending a rejection letter with details of how to get past the block).

⁶⁸ As noted above, the term commercial is defined in the Act, and the FTC is required to issue regulations related to that definition. See *supra* para. 11.

⁶⁹ See, e.g., *CAN-SPAM Act*, Section 11(2).

⁷⁰ See *CAN-SPAM Act*, Section 11(2).

message sent is an MSCM. Commenters should address enforcement and administrative concerns associated with any Commission action taken to protect subscribers from unwanted MSCMs. We also ask whether the mechanisms described below might help alleviate those problems. In addition, we ask for comment on the effect either interpretation might have upon small businesses.

24 We seek comment on whether senders at this time have the practical ability to “reasonably determine” whether an electronic mail message is sent directly to a wireless device or elsewhere. Some MSM subscriber addresses might be identifiable if they use a phone number in front of a reference to an Internet domain of a recognizable wireless carrier. For example, “2024189999@[wireless company].com” would be such an address. However, we understand that other MSM subscriber addresses do not have such easily distinguishable addresses, such as “nickname@[wireless company].com.” Moreover, as technology evolves, the options available for accessing and reading electronic mail messages from mobile devices will only expand. Therefore, as required by the Act, we must “consider the ability of a sender” of a commercial message to “reasonably determine” that the message is an MSCM.⁵⁶

25 There appear to be a variety of mechanisms that, if implemented, could allow a sender to reasonably determine that a message is being sent to an MSM subscriber. We seek comment on the efficacy and cost considerations of each of the specific mechanisms identified below, as well as any reasonable alternatives, whether they are offered at the network level by service providers, at the device level by manufacturers, or even by other mechanisms involving subscribers themselves. We especially seek comment from small businesses on these issues. If wireless providers are to follow direction from subscribers as to which senders’ messages should be blocked or allowed to pass through any filter, we seek comment on whether such information about the subscribers’ choices is adequately protected. We seek comment on whether other protections are needed and what they might be.

26 In this section we focus on possible mechanisms to enable senders to recognize MSMs by the recipient’s electronic mail message address, specifically the Internet domain address portion.⁵⁷

27. *List of MSM domain names.* We seek comment on whether we should establish a list of all domain names that are used exclusively for MSM subscribers, to allow senders to identify the electronic mail addresses that belong to MSM subscribers. We note that this list would not include unique user names or mailboxes—rather, it would solely be a registry of a small number of mail domains to allow senders to identify whether any messages they were planning to send would in fact be MSCMs.⁵⁸ If an MSM provider were to use a portion of their domain exclusively for MSMs, the list would include the portion of its domain devoted to that purpose. In that case, we believe that a sender could consult such a list to reasonably determine if a message was addressed to a mobile service subscriber. We seek comment on whether it is

⁵⁶ CAN-SPAM Act, Section 14(c)

⁵⁷ See CAN-SPAM Act, Sections 3(5) and 14(d) (defining electronic mail address and mobile service commercial message)

⁵⁸ The unique user name or mailbox is commonly referred to as the “local part” of the electronic mail address. See CAN-SPAM Act, Section 3(5).

and how such a registry might be funded.⁶⁴ In particular, could the confidentiality of MSM subscriber electronic mail addresses be adequately protected if maintained on a widely-accessible list? We seek comment on the burdens on small businesses to participate in such a registry. We seek comment on whether the establishment of a registry of electronic mail addresses could result in more, rather than less, unwanted electronic mail messages being sent to those addresses.

30. *MSM-only domain name* We seek comment on whether it would be possible and useful to require the use of specific top-level and second-level domains, which form the last two portions of the Internet domain address. For example, could we allow carriers to use a top-level domain, particularly the ".us" country-code top-level domain, and require that to be preceded by a standard second-level domain (such as "<reserved domain>" for mobile message service)? Under such an approach, MSM providers wireless company ABC and wireless company XYZ would gradually transition the domain parts of their subscribers' electronic mail addresses to "@[wireless company ABC] <reserved domain>.us" and "@[wireless company XYZ].<reserved domain>.us" respectively. Could carriers or other parties subject to the Commission's jurisdiction implement such solutions independently, or would such approaches require cooperation of entities not generally under our jurisdiction? We seek comment on the burdens on small businesses to use such domain names.

31. *Common MSM subdomain names.* We seek comment on whether we should require one portion of the domain to follow a standard naming convention to be used for all MSM service, or whether each carrier could choose its own naming convention within its own domains, as long as it was only used for such service. We note that one apparently significant difficulty with this approach is that entities that do not provide MSM service might also adopt such names. Thus, the sender might not be able to distinguish those addresses to which sending an MSCM was prohibited from some other addresses to which it is not prohibited. We seek comment on these and any other domain name-based approaches, their respective merits, and their practicality. In addition, we seek comment as to the effect a domain-name based approach will have on small communications carriers and whether there are less burdensome alternatives for such businesses.

b. Challenge and Response Mechanisms

32. As an alternative, we seek comment on whether we should require wireless providers to adopt mechanisms that would offer what is known as a "challenge-response" system. A challenge-response mechanism sends back a challenge that requires a response verifying some aspect of the message. It is our understanding that technical mechanisms exist that could automatically hold a message and send a response to the sender to let the sender know the message was addressed to an MSM subscriber.⁶⁵ For example, such technology might either ask for confirmation from the sender before forwarding the message to the intended recipient, or just return the first message from a sender with a standard response noting that the intended

⁶⁴ We note that unlike telephone numbers allowed on the do-not-call registry, which does not include business telephone numbers, the electronic mail addresses protected under the CAN-SPAM Act include all types of accounts.

⁶⁵ "Challenge system for e-mail is spam foe," Diaz, S., San Jose Mercury News (Jan. 25, 2004) <www.contracostatimes.com/mld/cctimes/business/7792935.htm>

industry practice for providers to employ subdomains⁵⁹ that are exclusively used to serve their MSM subscribers that distinguish such customers from other customers. For example, if a company offers both MSM and non-MSM services, does it assign subscribers to those different services the same or different domain names for their addresses? If not, we seek comment on whether we should require MSM providers to do so. We seek comment on whether using exclusive subdomain names should be required for all MSM service, or whether we should require carriers to offer subscribers the option of using such a name.

28 In connection with this approach, we seek comment on whether we should establish such a list and prohibit the sending of commercial electronic mail messages to domains on that list as violations of the Act. We seek comment on what steps the Commission may take to encourage or require the use of domain name oriented solutions by entities subject to our jurisdiction.⁶⁰ Further, we seek comment on what steps the Commission could take to facilitate these solutions through interaction with industry and other entities not directly regulated by the Commission. We seek comment on any practical, enforceability, cost or other concerns related to establishing such a list. We seek comment on how it might be established, maintained, accessed and updated. We seek comment regarding any burdens on small business owners who advertise using electronic mail to check such a list in order to comply with the Act.

29 *Registry of individual subscriber addresses* We seek comment on whether we should establish a limited national registry containing individual electronic mail addresses, similar to the national "do-not-call" registry.⁶¹ The FTC is tasked with reviewing how a nationwide marketing "Do-Not-E-Mail" registry might offer protection for those consumers who choose to join.⁶² Would a similar registry just for MSM addresses be consistent with the Act in general and with the greater protections provided in section 14(b)(1) for MSM subscribers? If the FTC implements a registry, how would ours differ? We seek comment on any practical, technical, security, privacy, enforceability, and cost concerns related to establishing such a registry.⁶³ In particular, we seek comment on how it might be established, maintained, accessed and updated. We seek information about the volume of addresses potentially included in such a registry, how MSM providers could verify that submitted addresses were only for MSM service,

⁵⁹ Domain name is defined in the CAN-SPAM Act as "any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet." *CAN-SPAM Act*, Section (3)(4). Typically an enterprise will register a second-level domain name with the registrar for a top-level domain (e.g., ".com" or ".net" or ".gov") to create the domain administered by the enterprise (e.g., *uscourts.gov*). By subdomain name we mean a further subdivision by the enterprise of its domain, identified by the characters to the left of the enterprise's domain name. For example, in the address "example@cadc.uscourts.gov" the subdomain name would be the "cadc" portion of the address.

⁶⁰ See *CAN-SPAM Act*, Sections 3(5) and 14(d) (defining electronic mail address and mobile service commercial message).

⁶¹ The national do-not-call registry was established to help consumers avoid unsolicited telephone calls. See Do-Not-Call Implementation Act, Pub. L. No. 108-10, 117 Stat. 557 (2003), *codified at* 15 U.S.C. § 6101 (*Do-Not-Call Act*).

⁶² *CAN-SPAM Act*, Section 9 (the FTC is required to report to Congress on this topic by June 1, 2004). See also Request for Information: Federal Trade Commission's Plan for Establishing a National Do Not E-mail Registry (February 23, 2004), <www.ftc.gov/opa/2004/02/dnem.htm>

⁶³ Note that all of these categories, except for cost, are items Congress has asked the FTC to discuss with regards to the Do-Not-E-Mail Registry. See *CAN-SPAM Act*, Section 9(a)(2).